양자암호장비 이기종 시스템 연동을 위한 양자키관리 시스템 개발

심규석, 이원혁
한국과학기술정보연구원

{kusuk007, livezone}@kisti.re.kr

Development of Quantum Key Management System for Interoperability of Quantum Cryptographic Devices

Kyu-Seok Shim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

양자암호통신망을 구축하기 위해 다양한 양자암호장비가 구성되어야한다. 양자암호장비에는 대표적으로 양자키분배장치(QKD, Quantum Key Distribution), 양자키관리 시스템(QKMS, Quantum Key Management System), 양자암호모듈(QENC, Quantum Encryptor) 등이 있다. 대표적인 구성요소는 세가지의 장비이지만 각 장비를 개발한 벤더사가 다르고, 현재 각 장비에 대한 인터페이스 표준이 적립되고 있으므로 이기종 장비에 대한 연동이 어려운 환경이다. 따라서 본 논문에서는 양자키분배 장치와 양자키관리 시스템간의 이기종 시스템 연동을 위한 양자키관리 시스템 기능을 개발하고 증명한다. 양자키관리 시스템의 기능을 수행하는 블록 중 이기종 시스템 연동을 위한 블록 및 각 블록에서 이기종 시스템 연동을 위한 기능 개발 내용을 소개한다.

Ⅰ. 서 론

양자컴퓨팅 시대에 맞춰 네트워크 보안은 양자컴퓨팅에 대비하여 새로운 보안체계를 구축하는데 초점을 맞추고 있다. 그 중 가장 유력한 보안체계는 양자키분배장치(QKD)를 기반으로 한 양자암호통신이다. 양자암호통신은 Alice 와 Bob 간의 양자키분배장치에서 생성한 대칭키를 이용하여 데이터를 암복호화하는 암호체계이다. 양자키분배장치에서 대칭키를 생성할 때 양자역학적 원리를 이용하여 도청자(Eve)가 도청을 할 시 Alice 와 Bob 측에서 도청유무를 판단할 수 있고, 도청이라 판단된 키를 사용하지 않음으로써 암호데이터 손실을 예방할 수 있다[1].

양자암호통신을 구성하기 위해서는 언급한 양자키분배장치 뿐만 아니라 양자키관리 시스템, 양자암호모듈 등이 필요하다. 양자키관리 시스템은 양자키분배장치에서 생성된 대칭키를 저장하고, 양자암호모듈에게 공급하며, 장거리 떨어진 노드들에게 키를 전달하며 대칭키의 라이플사이클을 관리하는 역할을 수행하면서 양자암호통신망을 구축하는데 필수적인 구성요소이다. 마지막으로 양자암호모듈은 양자키관리 시스템으로부터 키를 공급받아 데이터를 암복호화하는데 필요한 구성요소이다[2].

양자암호통신망을 구축하기 위한 세가지 구성요소는 필수적이다. 그러나 각 장비를 연동하기 위한 인터페이스는 표준화가 진행중이지만 현재까지 개발된 장비는 서로 다른 장비를 연동하지 못하는 한계가 있다. 따라서 현재 대규모 양자암호통신망을 구축하기 위해서는 하나의 벤더사로 통일해야만하고, 그렇다면 확장성이 매우 낮아지는 문제가 발생한다. 따라서 본 논문에서는 서로 다른 양자키분배장치를 하나의 양자키관리 시스템으로 연동할 수 있는 기능을 제안한다.

본논문에서는 본장 서론에 이어, 본론에서 서로 다른 양자키분배장치와 양자키관리 시스템 간의 연동방법에 대해 제안하고, 결론을 끝으로 논문을 마친다.

Ⅱ. 본론

본논문에서는 이기종의 양자키분배 장치를 동일한 양자키관리 시스템과 연동하여 양자암호통신망의 확장성을 높이기 위한 양자키관리 시스템 기능을 제안한다. 양자키관리 시스템은 그림 1 과 같이 10 가지 모듈로 구성되어 다양한 기능을 수행한다. 특히 키관리모듈(KMA, Key Management Agent), 키공급모듈(KSA, Key Supply Agent), 키전달모듈(KRA, Key Relay Agent)는 양자키관리 시스템에서 키 저장, 공급, 전달의 핵심기능을 수행한다[3].

양자키관리 시스템이 이기종 양자키분배 장치와 연동하기 위해서는 키관리모듈, QKDE manager, QKD Protocol Abstraction Layer 등에서 기능을 지원해야한다. QKDE Manager 는 QKD 요소들을 제어 관리하는 역할을 수행하며, 성능 및 장애 정보를 수신한다. QKD Protocol Abstraction Layer 는 다양한 QKD 와의 연동을 위한 Interface 기능을 수행하고, 마지막으로 키관리모듈은 양자키관리 정책 설정, 조회, 생애주기 관리, 키 동기화 기능을 수행한다.

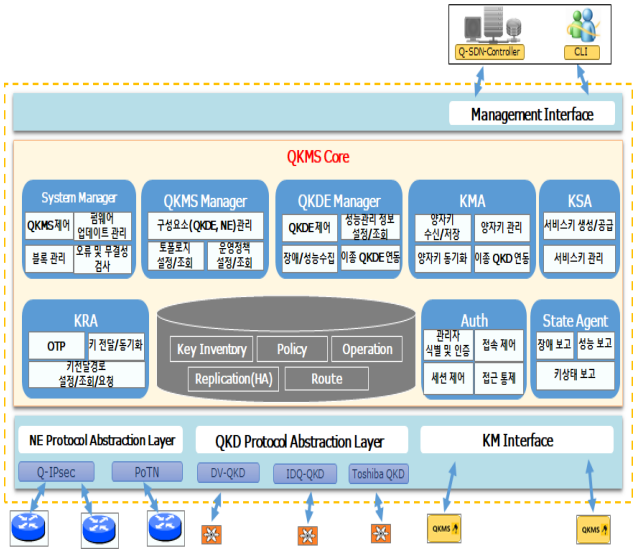

그림 1 양자키관리 시스템 구조

QKDE Manager 의 기능에는 이종 QKD 정보관리 기능이 포함된다. 서로 다른 QKD 정보를 관리하는 기능으로 이종 QKD 를 관리할 수 있는 통합구조로 Database 를 구성하여 이종 QKD 에 대한 정보를 관리한다. 이종 QKD 정보 관리를 위한 테이블 구조는 다음과 같다.

표 1 이기종 QKD 정보 관리를 위한 테이블 구조

	Desc	Type
QKDE_ID	QKDE UUID	BINARY(16)
QKDE_NAME	QKDE 이름	VARCHAR(64)
QKMS_ID	QKMS UUID	BINARY(16)
STATE	0: Normal 1: Abnormal	TINYINT(1)
VENDOR_ID		VARCHAR(128)
PRODUCT_ID		VARCHAR(128)
MODULE_PATH	SO 파일 경로	VARCHAR(256)
QKDE_ADDR	QKDE IP 주소	BINARY(16)
QKDE_PORT	QKDE 제어 포트	INT(11)
QKDE_MGMT_NAME	QKDE 관리용 이름	VARCHAR(64)

QKD Protocol Abstraction Layer 모듈에서는 QKDE 정보를 조회하고 제어 명령을 전달하는 기능을 수행한다. 기본적인 기능은 QKD 에서 수신한 양자키를 KMA 로 전달하는 기능이고, 추가적으로 QKD 의 장애, 성능 정보를 조회하는 기능을 제공한다. 따라서 이기종 QKD 와 연동하여 양자키를 수신받아 KMA 로 전달해야하며, 인터페이스를 통해 장애, 성능 정보를 제공할 수 있는 기능이 구현된다.

마지막으로 KMA 는 양자키 관리에서 가장 핵심 기능으로 키를 저장하고, 동기화 및 자원부족시 대처 등의 역할을 수행하며 이기종 QKD 연동을 위해 이종 QKD 지원 통합 양자키관리 기능을 포함한다. 이기종 QKD 지원 통합 양자키를 관리하는 기능으로 이기종 QKD 에서 수신한 양자키를 관리할 수 있는 통합 구조로 Database 로 구성하여 양자키를 관리한다. 이기종 QKD 지원 통합 양자키 관리를 위한 테이블 구조는 다음과 같다.

표 2 이기종 QKD 지원 통합 양자키 관리를 위한 테이블 구조

	Desc	Type
Q_KEY_ID	양자키 UUID	BINARY(16)
TIME	생성시간	BIGINT(20)
PEER_QKMS_ID	상대편 QKMS UUID	BINARY(16)
STATE	0: Pre-Activation 1: Active 2: Unavailable 3: Deactivated 4: Destroyed	TINYINT(1)
Q_KEY	양자키(Base64)	VARCHAR(128)

양자키관리 시스템의 모듈 중 위 세가지 모듈에 이기종 QKD 연동을 위한 기능을 구현함으로써 양자암호통신망 확장성을 증가시켰다.

Ⅲ. 결론

양자암호통신망을 구축하기 위해서는 다양한 벤더사, 다양한 장비들이 연동되어야 확장성 높아 질 수 있다. 따라서 양자키관리 시스템에 이기종 QKD 연동을 위한 기능을 구현하였다. 양자키관리 시스템과 양자키분배장치간에 인터페이스는 표준을 적용한다하더라도, 양자키관리 시스템에서 해당 장비를 구분하고, 키를 수신할 수 있는 기능이 필요하다.

향후 계획으로는 두 종류이상의 양자키분배장치를 직접 연동하여 키 전달하는 과정을 시험하고, 검증할 계획이다.

ACKNOWLEDGMENT

이 논문은 2024 년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다. (과제번호: K24L4M1C2)

참 고 문 헌

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[2] 심규석, 김용환, 이찬균, 이원혁. “KREONET 양자암호통신 환경에서 양자키 관리 시스템을 위한 양자키 저장 관리 모듈 설계 및 검증”, 2022 년 한국통신학회 동계학술대회

[3] Shim, Kyu-Seok, Yong-Hwan Kim, and Wonhyuk Lee. "A design of secure communication architecture applying quantum cryptography." Journal of Information Science Theory and Practice 10.spc (2022): 123-134.